King County	Department of Adult and Juvenile Detention All Divisions General Policy Manual	
	Chapter 1 **Administration and Personnel Management**	
1.03.054, Protection of Criminal Justice Information	Approved By:	Director John Diaz
	Effective Date:	June 08, 2022
	Reviewed By:	PRC, WACIC TAC
	Review Date:	May 26, 2022
Distribution:	Document Code No.	

Purpose
To provide guidance for department personnel, support personnel, and private contractors/vendors for the protection of Criminal Justice Information (CJI). All physical and logical access must be properly documented, authorized, and controlled on devices that store, process, or transmit unencrypted CJI. This policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from internal and external threats.

Policy
The protection of department facilities and sensitive CJI information secured within shall be in compliance with state, federal law, and county guidelines.

References

Federal:	FBI CJIS Security Policy
WSP:	ACCESS Manual
	Physical Protection Policy Template
County:	King County IT Governance Policies, Standards, and Guidelines
	Acceptable Use of IT Assets Policy (ITG-P-08-02-01)
Department Polices:	1.01.011, Facility Tours (Adult Division Policy)
	1.03.016, Background Investigations
	1.03.049, Background Reviews for ACCESS/WACIC
	1.03.052, Criminal Justice Information Systems
	4.01.008, Identification for Access to Department Facilities (Adult Division Policy)

Definitions
Authorized Personnel: Personnel that have department issued identification granting access to physically secure non-public locations and certified by Washington State Patrol (WSP) to access CJI information.
Criminal Justice Information (CJI): All Federal Bureau of Investigations (FBI) Criminal Justice Information Services (CJIS), Washington State Patrol (WSP) or other law enforcement agency provided data including, but not limited to biometric, identity history, biographic, property, and case/incident history.
Department Escort: Authorized Personnel responsible for accompanying visitors who do not have authorized access to CJI anytime they are within a physically secure location. The use of

cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Physically Secure Location: A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas shall be identified with a sign at the entrance.

Visitor: A person who is not employed by the department, and who does not have department issued identification granting access to the physically secure location within a facility.

General Guideline:

1. The Department will control physical access by authenticating visitors before authorizing escorted access to a physically secure location. The Department shall escort visitors at all times and monitor visitor activity.

A. Visitors shall:

1. Check in before entering a physically secure location by:
   a. Being logged in on JMS visitor/contact record by department staff at the point of entry to secure areas.
   b. Check out a visitor badge
      1) The visitor badge number shall be documented on the JMS visitor record.
      2) The visitor badge shall be worn on approved visitor's outer clothing (front, upper torso) and returned at the end of the visit.
   c. Check in multiple times if visiting multiple physically secured areas not adjacent to each other, each having individual perimeter security.
2. Be accompanied by a department escort at all times, to include delivery or service personnel.
3. Show department personnel a valid form of photo identification when requested.
4. Not be allowed to view screen information, mitigating shoulder surfing of CJI.
5. Individuals not having legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, uniform staff shall be notified or call 911.
6. Not be allowed to sponsor another visitor.
7. Not enter any secure area, to include physically secure locations, with electronic devices unless approved by the Division Major/Deputy Division Director (or higher authority), to include cameras and mobile devices.
8. Not take photographs without written permission of the Division Major/Assistant Division Director (or higher authority) following department policy 1.01.011, Facility Tours.
9. All requests by groups for tours of a department facility shall be referred to the Division Major/Assistant Division Director for scheduling following department policy 1.01.011, Facility Tours.

B. Authorized Physical Access and Personnel

1. Only authorized personnel shall have access to physically secure non-public locations.
   a. Any Non-Criminal Justice Agency (NCJA), like county IT, who require frequent unescorted access to restricted area(s) shall be required to establish a Management

Control Agreement between the department and the NCJA. Each NCJA employee with CJI access shall appropriately have state and national fingerprint-based record background check prior to restricted area(s) access being granted.

b. Private contractors or vendors, who require frequent unescorted access to restricted area(s), shall be required to establish a Security Addendum between the department and each private contractor. Each private contractor shall appropriately have a state and national fingerprint-based record background check prior to this restricted area access being granted.

2. The department shall maintain a current list of authorized personnel.
3. All access points to secure areas of DAJD facilities shall by controlled by the Department and authority to access secure areas shall be verified before granting access.
4. All areas that contain, transmit or display CJI shall be monitored and have physical access controls.
5. All authorized personnel shall take necessary steps to prevent violations of CJI policies.
6. All authorized personnel shall:
   a. Meet the minimum personnel screening requirements prior to CJI access following policy 1.03.049, Background Reviews for ACCESS/WACIC.
   b. Complete Security Awareness Training.
      1) All authorized department and NCJA personnel shall receive state approved Security Awareness Training within six months of being granted duties that require CJI access and every two years thereafter. Training logs shall be maintained by the TAC .
      2) Security Awareness Training shall, at a minimum, cover areas specified in department policy regarding CJI security (1.03.052, Criminal Justice Information Security).
   c. Be aware of who is in their secure area before accessing CJI.
      1) Take appropriate action to protect all CJI.
      2) Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by unauthorized persons.
   d. Properly protect individually issued keys, proximity cards, computer account passwords, and other security measures.
      1) Report loss to a supervisor.
         a) Supervisors shall make the appropriate contacts to have authorized credentials, such as proximity cards de-activated and/or door locks rekeyed, as necessary.
      2) Take appropriate measures to safeguard passwords, Personal Identification Numbers (PIN), Security Tokens (Smartcard or proximity cards), and all other facility and computer systems security access procedures.
         a) Sharing this information, even with other authorized personnel is strictly prohibited.
      3) Failure to follow the above steps shall be forwarded to the Internal Investigations Unit (IIU) for investigation.
   e. Ensure King County IT Governance Policies, Standards, and Guidelines are properly followed to ensure CJI is protected from viruses, worms, Trojan horses, and other malicious code. This shall include not using personally owned devices on department computers with CJI access.

f. Protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non-secure location, appropriate controls shall be utilized to prevent data compromise and/or unauthorized access.
g. Encrypt emails, when electronic mail is allowed, to transmit CJI-related data as such in the case of Information Exchange Agreements.
    1) If CJI is transmitted by email, the email must be encrypted, and email recipient must be authorized to receive and view CJI.
h. Report any physical security incidents to the department's IT Point of Contact (POC) via chain of command to include but not limited to loss of laptops, smartphones, thumb drives, and CDs/DVDs containing CJI.
i. Only release hard copy printouts of CJI to authorized, vetted personnel in a secure envelope and dispose of CJI in accordance with policy 1.03.052, Criminal Justice Information Systems.
j. Log all transfers of CJI to appropriate entities on the Secondary Dissemination Log following policy 1.03.052, Criminal Justice Information Systems.
k. Keep appropriate department security personnel informed when CJI access is no longer needed.
l. In the event of ended employment, surrender all property and access managed by the department, local, state, or federal agencies. Ensure perimeter security doors securely lock after entry or departure. Never leave perimeter doors propped opened and take measures to prevent "piggyback" entries.

C. Penalties

1. Violation of any of the requirements in this policy by any personnel shall result in appropriate disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination.
2. Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.